



Criminal Division

Christopher A. Wray
Assistant Attorney General, Criminal Division
U.S. Department of Justice

Remarks* to the
AMERICAN COLLEGE OF TRIAL LAWYERS

Phoenix, Arizona
March 6, 2004

*Mr. Wray frequently speaks from notes and may depart from the speech as prepared.

Thank you for that kind introduction and for the invitation to be here. It is a real honor to address this distinguished group at this particular time – a time frankly unprecedented in our country’s history – when lawyers, in the criminal justice system and elsewhere, are stepping forward and leading in new ways.

Over the past two years, the Department of Justice has undergone a paradigm shift in our mission and our methods. It started in the Fall of 2001, which marked a historic turning point for this country. In one tragic morning, the World Trade Center was attacked and destroyed by terrorists. The attacks of September 11 took over 3,000 innocent lives and forever changed the way that Americans think about security and the way that our government must ensure it. Just one month later, the Enron Corporation began to implode. By December, Enron had filed for bankruptcy, jarring worldwide confidence in our markets, causing financial ruin to scores of Americans and delivering a serious blow to our economy.

These events starkly demonstrated to all Americans the grave threats that terrorism and corporate fraud pose to our lives, our livelihoods, and our way of life. This Administration has responded aggressively to these threats. And thankfully, since September 11, we have not seen another major terrorist attack on American soil. And our markets are regaining their strength; our economy continues to grow and add jobs.

We have emphasized two themes in our efforts. First, we are pursuing “real-time enforcement” against terrorists and perpetrators of corporate fraud. In other words, we are playing strong offense, not just defense. Second, we are seeking ways to enlist the private sector – and the public generally – in our efforts.

Despite obvious differences between our two top priorities of terrorism and corporate fraud, our approach to each represents something of a sea change from the past and shares these two fundamental features.

I. REAL-TIME ENFORCEMENT

Terrorism

Like all of you, I remember where I was on September 11, when I first learned of the attacks on the World Trade Center and the Pentagon. I vividly recall the chill that I felt as I watched television footage of the wounded Manhattan skyline from the Department’s Command Center. I will never forget the first conversations I had with my wife and children after learning of the tragedy, or the grim faces of my colleagues at the Justice Department.

Just as memorable, though, were the burdens of the next few months. All of us in the Department jolted each time our pagers went off – day or night. Our adrenaline raced with every report of white powder in someone’s mail. Every airplane pilot who did not promptly respond to radio calls brought a cold knot to our stomachs. We were determined not to miss something that would cost more innocent lives, so each of these incidents made us think with dread, “not again.”

Two years later, it’s easy to be lulled into complacency about the terrorist threat. As September 11 recedes in time, it’s natural for it to begin to resemble some hazy, horrible nightmare. But it was no bad dream. Every morning, those of us in the law enforcement, intelligence and military communities confront the threat on a very real basis when we meet to review the daily intelligence. We know that there are many who would gladly take the place of the September 11 hijackers, who are just as intent on killing more innocent people. These guys are sophisticated, cunning, disciplined, and utterly committed to mass murder. Figures like Usama bin Laden exhort their followers to fulfill their holy duty of killing Americans. Our enemy still has the desire and the capability to strike the U.S. with little or no warning. According to intelligence estimates, *15,000 to 20,000* terrorists have been trained in Al Qaeda’s camps in Afghanistan since bin Laden established them in 1996. We need only recall how much harm 19 caused on 9/11 to understand the threat that any one of these thousands poses.

This is especially true when we know that Al Qaeda remains intent on obtaining and using chemical, biological, radiological and nuclear weapons of mass destruction. And the threat is not limited to Al Qaeda. The steady growth of bin Laden’s anti-American beliefs through the wider Sunni extremist movement and the broad dissemination of Al Qaeda’s destructive expertise ensure that a serious threat is here to stay – with or without Al Qaeda in the picture.

Despite these challenges, we’re making significant progress and scoring key victories in the war on terror. Since September 11, we have charged 300 defendants as a result of terrorism investigations. To date, almost 170 have already been convicted. We have broken up terrorist cells in Buffalo, Charlotte, Seattle, Portland, and – just this week – northern Virginia. Through unprecedented interagency and international cooperation, nearly two-thirds of Al Qaeda’s leadership worldwide has been captured or killed. Most importantly, since September 11, we have not seen another major terrorist attack on American soil.

Pursuing and prosecuting terrorists *after* an attack is part of our mission but it’s not the focus of our efforts. A good defense is important, but it is not enough. We must be *proactive*, not *reactive*, and take the fight to the enemy. If we are left picking up the pieces after an attack, then we have failed in our preventive mission. That sounds

obvious enough, but old models of law enforcement and deterrence won't work with adversaries who not only accept, but glorify killing themselves in the course of attacking thousands of innocent people. We need to play offense – disrupting terrorism through aggressive investigation, comprehensive intelligence gathering, and real-time analysis of that data.

By far, the single greatest boost to real-time enforcement against terrorism has been the PATRIOT Act's removal of the barrier between law enforcement and intelligence efforts on international terrorism investigations. Thanks to the elimination of this "wall," that Jim Comey discussed yesterday, we are far better equipped to "connect the dots" in real time to identify and disrupt terrorist threats. The post-9/11 FBI fully integrates intelligence and law enforcement capabilities to protect American lives.

Aided by our new ability to share information with our colleagues in other agencies, the government is able to use every tool in our arsenal to deter, disrupt, and defeat terrorists – from intelligence collection to immigration exclusion or deportation to criminal prosecution to diplomatic pressure to military force. On a personal note, I can tell you that the head of the Criminal Division's job has changed dramatically from that of my pre-9/11 predecessors: Not a day goes by that I or someone on my behalf isn't in operational discussions with counterparts at the CIA, the Defense Department, the NSC, and, of course, the new Department of Homeland Security.

Our offensive strategy extends beyond the actual perpetrators of violence to their supporters as well. We must address the entire terrorist network, from the front-line killers to the fundraisers, to maximize our chances of taking out those upon whom terrorist operations depend. Another way to see and understand our approach is to think of the chronology of a terrorist plot, a continuum from idea, to planning, to preparation (including fundraising and other support, training, reconnaissance and so on) to execution and attack. We need to strike earlier on that continuum – we'd rather catch terrorists with their hands on a check than on a bomb.

Even Jeffrey Battle, a member of the terrorist cell broken up in Portland, understood the importance of the PATRIOT Act and its real-time enforcement effect. In a recorded conversation with an FBI informant, Battle explained why his enterprise was not as organized as he thought it should have been because – and I'm quoting him now:

“. . . we don't have support. Everybody's scared to give up any money to help us. . . . Because that law that Bush wrote about . . . Everybody's scared . . . He made a law that says for instance I left out of the country and I fought, right, but I wasn't able to afford a ticket but you bought my plane ticket, you gave me the money to do it . . . By

me going and me fighting, by this new law, they can come and take you and put you in jail.”

Within the realm of criminal prosecution, we will use any offense that the law and the evidence support – a variation on the “spitting on the sidewalk” approach Bobby Kennedy’s Justice Department used against the Mob – to disrupt terrorist activity. We’re using every tool the laws, the evidence, and the Constitution allow us – the public deserves no less.

Not infrequently, we’ll charge terrorism suspects with non-terrorism crimes – not because their links to terrorism are lacking. In certain cases, evidence of terrorist connections or activity may not be sufficient to prove a terrorism crime beyond a reasonable doubt, or proving some criminal offenses may require the disclosure of sensitive sources or classified information. In situations like these, the best alternative from a national security perspective is to get the defendant off the streets by bringing other charges against him – charges that can be proved beyond a reasonable doubt and do not require the disclosure of sensitive information. This is often the best way to achieve our most important objective: preventing terrorist attacks.

We are also using the legal tools available to us to strengthen the country’s anti-terrorism infrastructure. For example, hundreds of airport and seaport workers have been charged with falsifying documents like Social Security applications and violating immigration laws. At Dulles and Reagan airports alone, 94 workers were arrested on those kinds of offenses. Even where not tied to terrorism, these cases address dangerous vulnerabilities that terrorists seek to exploit.

This kind of prompt, proactive, and preventive strategy is the only way we’re going to win the war on terror.

Corporate fraud

Speed also matters in corporate fraud investigations. One of our principal aims in these cases is to disgorge ill-gotten gains from the guilty parties and restore them to investors and other victims, before they can be dissipated or stashed in some offshore account. Where executives have committed fraud, protecting the corporation and the public often requires quick action to remove wrongdoers from their positions so they can’t run the company further into the ground. Sophisticated financial crimes take a long time to investigate thoroughly, but the public simply can’t wait years for law enforcement to take action. A rapid, real-time response to allegations of fraud is critical to maintaining confidence in the markets and the economy as a whole.

In response to the parade of corporate scandals that began with Enron in 2001 and continued with other high-profile cases like WorldCom and Adelphia in 2002, the President created the Corporate Fraud Task Force, a group of top federal law enforcement and regulatory agencies. The combined efforts of prosecutors, the FBI, the SEC, the CFTC, the IRS, and a number of others have demonstrated our commitment to taking swift and decisive action against corporate fraud.

As someone who's seen corporate fraud investigations from both the defense side and as a line prosecutor, I would characterize the impact of this commitment as truly dramatic. Criminal charges are often now brought months, not years, after investigations begin. Just since its inception in the Summer of 2002, through the end of last year, the Task Force has been involved in over 350 criminal investigations. By the end of 2003, those investigations had resulted in criminal charges against more than 660 defendants accused of corporate fraud. So far, more than 250 of those defendants have already been convicted on corporate fraud charges.

Our new strategy of "segmenting" investigations is a perfect illustration of the paradigm shift in law enforcement. Because these cases are so complicated, we could easily spend years investigating them. But we don't have years to assemble the "perfect" case, where each possible defendant and all wrongdoing are compiled into a single mother-of-all indictments or enforcement action. Rather, investigators and attorneys seek to take action as swiftly as the evidence will allow. This "real-time" enforcement is best accomplished when distinct cases, which comprise a separate segment of conduct involved in a larger investigation, are brought as soon as they are ready and as quickly as possible.

For example, in the Enron investigation, we have systematically unraveled the most complicated corporate scandal in history. So far, 29 defendants have been charged – but not, as might have occurred before, in one big case. Arthur Andersen has already been tried and convicted in a one-count conspiracy case. Several Enron executives, including the CFO, have already pled guilty to participating in parts of the massive fraud that destroyed Enron. That step-by-step approach led to the indictment of former CEO Jeff Skilling earlier this year. Although the investigation has been going on for more than two years now – and remains very active and ongoing – those kinds of results are lightning-fast compared to such investigations not long ago.

In the case of Adelphia, one of the country's largest cable operators, investigators began looking into allegations of accounting fraud in April 2002, days after the allegations first surfaced. They quickly uncovered a management scheme to deceive the public about the company's performance. Within four months, from April to July, the

CEO and four other top executives were in handcuffs. Four defendants are being tried right now in New York.

In the WorldCom investigation, the SEC filed its civil enforcement action the day after WorldCom revealed its improper accounting for billions in expenses. Prosecutors immediately began an intensive criminal investigation. Although it soon became clear that accounting irregularities extended to many aspects of WorldCom's financial reporting, the prosecutors stayed focused on the problems that appeared most likely to support criminal charges, and charged the CFO and Controller just five weeks after the revelation of fraud. The CFO is now cooperating with the Government and pled guilty this past Tuesday. That cooperation helped secure the indictment of the CEO himself, Bernie Ebbers.

And in the HealthSouth investigation, within the first seven months alone, the Department had charged 16 people – including 3 of its former CFOs and the CEO and Chairman himself, Richard Scrushy. Fourteen of them pled guilty in that same stretch.

These real-time enforcement successes, and many others like them, would not be possible without the powerful combination of resources and expertise established by the creation of the Corporate Fraud Task Force. And we find it encouraging that confidence in corporate America seems to be returning and the economy recovering.

II. COMMUNITIES AS FORCE MULTIPLIERS

No matter how many government agencies we bring to bear on terrorism and corporate fraud, however, and no matter how fast and well-integrated our efforts are, the truth is that we should not entrust our security and economic well-being to the government alone. The private sector – and the public generally – are themselves indispensable to our collective self-defense.

Terrorism

This is nowhere more true than in the war on terror. We're recognizing something now that the public in Israel has confronted for years in their country. Our enemy's ruthlessness and sophistication require all of us to be vigilant against threats to ourselves, our loved ones, and our communities. As Judge Young knows, were it not for the airline passengers and crew who confronted Richard Reid as he tried to ignite a bomb in his shoe, terrorists might have claimed yet more innocent lives. When Reid attacked the flight attendant who tried to stop him, another passenger reached over the seat to restrain Reid's arms. Others rushed to restrain his legs. Still others donated their

belts to tie Reid down. A doctor on board sedated Reid. Another passenger held a fire extinguisher as a weapon, guarding Reid for the rest of the flight. On that flight, every passenger was vigilant, every passenger was an air marshal, every passenger a hero. Because of their vigilance, 197 passengers and crew made it to the ground safely that day. Reid is now serving a life sentence in prison.

Public vigilance is also crucial because terrorists have gained footholds everywhere, even in our own backyards. People need to understand that terrorism is not a threat limited to places like downtown Manhattan or Washington, D.C. We've got terrorism cases or investigations pending in places like Idaho; Lackawanna, New York; Portland, Oregon; Minneapolis, Minnesota; and Tampa, Florida. And those are just some of the cases I can talk about. And the cells are hardly limited to aliens: Some of our own citizens are implicated. Just a few weeks ago, we teamed up with the military to catch a National Guardsman in Washington state now charged with trying to feed information to Al Qaeda. The arrest came as his unit was preparing for deployment to Iraq.

The aftermath of September 11 itself showed another, powerful way that the government and the private sector can partner in the war on terror. After the tragic attacks on that day, our first goal was to defuse the immediate threat: The 19 dead hijackers could well have had cohorts who were planning even more carnage. We had to reconstruct the hijackers' lives, to determine where they had lived, how they had supported themselves and – most ominously – whom they had contacted, who might still be out there, planning another deadly attack.

We quickly realized that the key to this effort was financial data. It's virtually impossible to live in Western society without leaving digital footprints. Every time you book a hotel or an airline reservation, you leave a mark. Every time you withdraw cash from an ATM, you have your picture taken. In virtually every activity we undertake in modern society, some entity, generally in the private sector and not the government, keeps track of it. So we staffed a special FBI unit with financial investigators and prosecutors and turned them loose on the puzzle.

Our experience taught us an important lesson: law enforcement cannot meet this type of challenge without effective cooperation and communication with our colleagues in the private sector.

Most of the records we needed were in the hands of third parties, many of them probably clients of yours, some in regulated industries that require certain safeguards as a condition of publicly disclosing information. We therefore estimated that the puzzle would take about six months of subpoenas and government analysis to solve. And we

weren't sure we could afford it to take that long. But, unexpectedly, we began receiving highly polished analysis from the private sector, whose members had taken the initiative to develop sophisticated algorithms to search their own records for information that they knew would help us.

In some ways, I suppose, this shouldn't have surprised us. The tragedy of 9/11 touched every American, but no group was as directly affected as the financial community, who lost so many colleagues and loved ones when the Twin Towers went down. These people were looking for every opportunity to help us. We're working to continue that terribly important collaboration as we look forward in the war on terror, beyond September 11.

Corporate fraud

On the corporate fraud front, assuring integrity in American business cannot be accomplished by the government alone either. We don't have enough agents and prosecutors to single-handedly eradicate all corporate fraud. So we are grateful for and encourage the efforts of many in corporate America to set higher ethical standards, to help identify corporate wrongdoers, and to protect shareholders' interests. We well understand that the executives charged in the Enron, Adelphia, and HealthSouth investigations do not represent corporate America. The vast majority of executives are of course honest and hard-working, and the vast majority of companies are of course law-abiding organizations that provide invaluable goods, services, and jobs.

Our aggressive new level of enforcement has given businesses a powerful incentive to develop their own responses to the challenge of higher ethical standards. Companies seem to be getting the message that cooperation is in their own self-interest, and they're maximizing that self-interest by coming up with new and innovative ways to assist the Government. For example, when the Enron Task Force uncovered criminal conduct on the part of certain employees of Merrill Lynch and Canadian Imperial Bank of Commerce (CIBC), those companies accepted responsibility for their employees' conduct and agreed to cooperate fully with the ongoing investigation, implement sweeping reforms to their internal processes, and be overseen by an independent monitor. Satisfied by this swift and wholehearted response, we agreed to defer prosecution – in other words, we promised not to prosecute those companies as long as they make good on their promises of cooperation and reform.

Less and less, but still too often, management decides to lay low and hope the crisis will blow over. When federal regulators or agents come knocking on a company's door, we expect truthful and forthcoming cooperation and diligent efforts to identify and correct problems, not denial or passive-aggressive obstinance and never obstruction.

And if we find significant fraud, we will ask why we had to knock on their door, rather than their coming to us in the first place.

The Sarbanes-Oxley legislation was an important component of the response to corporate fraud. But instead of relying only on new rules, we've responded with the massive and rapid enforcement effort that I've described. When you stop and think about it, good corporate citizens should welcome our enforcement-based approach because – unlike regulation – it targets the bad apples, not the whole barrel. Our efforts also help shore up confidence in the markets. By continuing to work with the Government to develop innovative ways to police themselves, companies can tamp down the call for even more stringent regulation and improve their own financial prospects by helping to restore confidence in our markets.

CONCLUSION

As I said earlier, these are unprecedented times but exciting ones to be a litigator for the Government. We are dealing with new challenges that demand new approaches. The issues we're grappling with today could not be more important – indeed many are matters of life and death – and they deserve our utmost attention.

I want to conclude by asking for your help in continuing to meet these challenges. After all, we share the same mission. Lawyers, in their various roles, have always played an influential part in shaping our society, ensuring our security and preserving our liberties. In our adversarial system, justice depends on effective advocacy, which each of you provides in your community. As leaders of the bar, your voices carry special weight in public discourse. Through the College, you provide a forum and encourage the discourse that is essential to a free, just and democratic society. These are the very things we at the Justice Department are working so hard to preserve.

Thank you for having me.